

REMARKS

The Applicants request reconsideration of the Final Rejection dated September 20, 2007.

Claims 17 and 29-31 are now pending, including new claims 29-31.

Claim 17 was finally rejected under 35 U.S.C. §103(a) as being unpatentable over Ho et al., U.S. Patent Publication No. 2004/0254934 (Ho) in view of Kavalam et al., U.S. Patent Publication No. 2005/0091658 (Kavalam), Wiik et al., U.S. Patent No. 5,260,551 (Wiik), Wang et al., U.S. Patent Publication No. 2004/0203589 (Wang) and Trossen et al., U.S. Patent Publication No. 2004/0153552 (Trossen).

The Applicants incorporate by reference each of the remarks previously advanced. Although the Applicants do not agree with the position taken by the Examiner in rejecting claim 17, to expedite prosecution, claim 17 has been amended as set forth above. A discussion of the amendments follows.

As finally rejected, claim 17 recited an access control system in which a plurality of storage devices for storing information resources and access controllers for controlling accesses to the information resources stored in the storage devices are connected with a network. Each access controller comprises an access restriction module, an access interception module, and an access control list update module. In the rejected claim, at least one of the access controllers has an updated access prohibition list and further comprises a distribution module configured to send out user information of access prohibited users, or an updated access prohibition list, to the other access controllers in response to an update, and the other access controllers comprise a list update module configured to receive the user information

or the updated access prohibition list and to update the access prohibition list thereof to include the received user information or updated access prohibition list.

To clarify the invention, claim 17 has been amended to positively recite that each access controller comprises a list update module configured to update the access prohibition list, and a distribution module. Further, claim 17 now recites that the distribution of at least one of the access controllers has an updated access prohibition list and is configured to send out the user information or the updated access prohibition list to the other access controllers in response to the access prohibition list of the sending access controller being updated. Further, in accordance with the positive recitation of the list update module, claim 17 has been amended to recite that the list update module of each of the other access controllers is configured to receive the user information or the updated access prohibition list and to update the access prohibition list thereof to include the received user information or updated access prohibition list.

In addition, the paragraph beginning "wherein the distribution module of each access controller" has been deleted as redundant.

Claim 17 has also been amended to require that, after the list update module of each of the other access controllers updates the access prohibition list thereof, the access control list update module thereof updates the access control list thereof according to the updated access prohibition list. Further, in response to completing the updating of the access control list thereof, each of the other access controllers notifies the sending access controller of the completion, and the list update module of the sending access controller deletes the user information or the access prohibition list thereof at a predetermined timing after receiving the completion

notifications from the other access controllers. None of Ho, Kavalam, Wiik, Wang, or Trossen discloses or fairly suggests the features of the claim as amended. The Applicants particularly direct the Examiner's attention to Fig. 10, and particularly steps Sa200 – Sa207. In these steps, as disclosed, access controller 200, access controller 300, and access controller 400 individually complete the update of the access control list thereof, and notify the completion to the sending access controller 100 in the preferred embodiment depicted in Fig. 10. Access controller 100 receives the notifications and deletes its own black list (access prohibition list) after receiving the completion notifications.

New dependent claim 29 further limits the access control system of claim 17 by requiring the sending access controller to be configured to send an instruction to each of the other access controllers for deleting the user information or updated access prohibition list sent thereto, the instruction being sent by the sending access controller to each of the other access controllers after receiving the notification of completion therefrom. Again referring to Fig. 10 as an example of support, the Applicants refer to step Sa208, instructing deletion of the black list to access controller 200, step Sa210, instructing deletion of the black list to access controller 400, and step Sa212, instructing deletion of the black list to access controller 300.

New dependent claim 30 requires each of the access controllers to manage a different respective information resource on the basis of at least one of the access control list and the access prohibition list in the access controller to control accesses from a client computer with user information. New dependent claim 31 requires each

of the access controllers to manage information resources in a different respective first network, wherein each of the first networks is coupled to a second network.

None of the applied references, or the other references of record, taken in proper combination with the applied references, is believed to disclose the features of claims 29, 30 or 31.

Accordingly, the Applicants request reconsideration of the rejection and allowance of claims 17 and 29-31.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Mattingly, Stanger, Malur & Brundidge, P.C., Deposit Account No. 50-1417 (referencing attorney docket no. MEI-101).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

/Daniel J. Stanger/

Daniel J. Stanger
Registration No. 32,846

DJS/sdb
(703) 684-1120